UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/884,672	06/19/2001	Tetsuya Noguchi	JP920000134US1	4503

7590 01/05/2005

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. Box 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/884,672	**Applicant(s)** NOGUCHI ET AL.
	Examiner Peter Poltorak	**Art Unit** 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 June 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-43 have been examined.

Priority

2. The effective filing date for the subject matter defined in the pending claims in this application is 06/20/2000.

Specification

3. The disclosure is objected to because of the following informalities: the statement "Note that this received public key is referred to as Kx rather that Kc here" *(pg. 30 last §)* suggests that Kc stands for a public key. However, in the earlier citations the specification suggests that Kc is a symmetric key and Kp is denoted as the public key.

   Appropriate correction is required.

Drawings

4. The drawings are objected to because of the following informalities: although pages 23-25 in the specification describe Fig. 5, the cited description does not allow clear understanding of the image in regard to the verification process and the meaning of the columns within the image. For example, it is unclear whether all of the columns should be of equal length if no tampering is detected.

5. Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be

notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

6. Claim 32 starts with "31." which seems to be an error and should be removed.

Claim Rejections - 35 USC § 112

> The following is a quotation of the first paragraph of 35 U.S.C. 112:
>
> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 9, 11, 21 and 23 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. The way that Kc is generated is critical or essential to the practice of the invention, but not included in the claim(s) and thus is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976).

8. Claims 9, 11, 21 and 23 contain the following limitation:

"The public key Kp is transmitted from the portable terminal to the personal computer of each user, then the personal computer of the other user generates a symmetric key Kc based on a second generation algorithm, while the personal computer of the one user generates the symmetric key Kc based on the second generation algorithm from information transmitted from the personal computer of the other user in cipher according to the public key; and thereafter both the personal computers send and receive data in cipher according to the symmetric key Kc".

The above limitation does not allow to determine how the Kc is derived, whether it is delivered encrypted with Kp, whether some other data is sent which allows personal computer of each user to derive the Kc or whether some other mechanism is employed for the personal computer to obtain the identical Kc.

Claims 33, 35, 38 and 40 are rejected by virtue of their dependence.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1-43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Claims 4, 16 and 28 recite: "establishing a serial sequence of operators that are composed of one or more of operators arranged in series, wherein the operators relate to the same or different one-way functions". The claims as cited allow for the "one of operator" to satisfy the claims' limitation. However, it is not clear how it is possible to arrange the "one of operator" (function) in series or to be used in a serial sequence of operators.

11. Claims 7 and 19 are not clear. The claims first introduce "an operator" followed by a plurality of operators", then "each operator". It is not clear to which operator "each operator" "each operator" refers, especially since no explicit relationship between "an operator" and "the operators" is established in the claim language.

12. The "verification data generation based on a first generation algorithm" statement in claims 1, 13, 25 and 30 is not clear. For purpose of further examination the statement will be treated as "a first generation algorithm is used to produce verification data generation".

13. The "symmetric key Kc based on a second generation algorithm" statement in claims 9-12 and 21-24 is not clear. For purpose of further examination the statement will be understood as "a second generation algorithm is used to produce symmetric key Kc".

14. The "cipher according to the public key" and the "cipher according the symmetric key Kc" statements in claims 9-12 and 21-24 are not understood. It is not clear whether claims refer that the keys are used to produce the cipher or to something else.

15. Claims 9-12 and 21-24 recite the method comprising a portable terminal and a personal computer that are owned by each user. It is not clear whether the portable terminal is owned by one user and the personal computer by another user or whether there are portable terminals and personal computers, wherein each set is owned by each user. In light of other limitations the examiner treats

the limitation (discussed above) as though it establishes two terminal/computer sets, wherein one set is owned by one user and another set by another user.

16. The limitation "a numeric on which the operator operates as in input of the operator" in claims 4, 6, 7, 16, 18, 19, 28 are not well understood. For further examination purposes the statement is understood as "a numeric as in input on which the operator operates".
17. Claims 9-12 are narrative in form and replete with indefinite and functional or operational language essentially transforming a product claim into a method claim. The structure, which makes up the device, must be clearly and positively specified. The structure must be organized and correlated in such a manner as to present a complete operative device.
18. Claims 31 and 32 are the same *(besides the number "31" preceding limitations of claim 32, see Claim Objections above).* The purpose of two identical claims is not understood.
19. Similarly, the purpose of two identical claims 41 and 42 is not understood.

Claims 2-3, 5, 8, 14-15, 17, 20, 24, 26, 29, 33-35, 37-39, 40, 43 are rejected by virtue of their dependence.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

20. Claims 1, 4-7, 13, 17-19, 25, 28-32, 36-37 and 43 are rejected under 35 U.S.C. 102(e) as being anticipated by *Vainio (Juha T. Vainio, "Bluetooth Security").*
21. As per claim 13 *Vainio* teaches Bluetooth authentication wherein a Device A sends RAND A to a Device B *(Fig. 6).* This reads on sending data for verification data generation from one data

send/receive device to the other send/receive device, wherein the two send/receive devices are mutually connected by an ad-hoc radio connection.

Furthermore *Vainio* teaches authentication function E1 in the Device A is used to create SRES' using RAND A *(Fig. 6).* This reads on generating verification data in the one data send/receive device, from the sent data for verification data generation based on a first generation algorithm.

Similarly, the Device B derives SRES using RAND A and applying E1 *(Fig. 6)*. This reads on generating verification data in the other data send/receive device from the received data for verification data generation based on the first generation algorithm.

Fig. 6 shows SRES being sent from the Device B to the Device, A which verifies whether SRES' and SRES match. This reads on determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually.

22. *Vainio* does not explicitly teach outputting the generated verification data to its own verification data output section by each of the devices. However, this feature is inherent. E1 represents the authentication function and generated output ends up in a (verification data output) section of the device comprising the E1.
23. Claims 1, 25, 30-32 and 43 are substantially equivalent to claim 13; therefore claims 1, 25, 30-32 and 43 are similarly rejected.
24. As per claim 17 *Vainio* teaches Bluetooth as a technology enabling devices to connect to each other and his discussion on authentication scheme is a generic discussion on how the devices authenticate with other device. The authentication scheme as disclosed in Fig. 6 is repeated numerous times.
25. As per claims 16 and 18 E1 function is defined as an operator operating on a numeric input RAND A, which is the data for verification data generation *(Fig. 6)*.
26. As per claim 19 *Vainio* teaches a plurality of operators that relate to mutually different one-way functions, e.g. E0 (fig. 5), E3 (fig. 4) and 21 (Fig.3)
27. Claims 4-7 and 28-29 are substantially equivalent to claims 16-19; therefore claims 4-7 and 28-29 are similarly rejected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

28. Claims 2-3, 14-15 and 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of Official Notice.

29. *Vainio* teaches an ad-hoc radio communication as discussed above. *Vainio* does not explicitly teach that the verification data is visual and auditory verification data.

    Official Notice is taken that visual and auditory verification data is old and well-known (e.g. Windows authentication visually and audibly notifies about a password being not valid). One of ordinary skill in art at the time of applicant's invention would use visual and auditory verification data to enhance system's usability.

30. Claims 8 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457).*

31. *Vainio* teaches data for verification data generation as discussed above. *Vainio* does not teach that the data for verification data generation is a public key of either data send/receive device. *Schneier* teaches the data for verification data generation, which is a public key of either data send/receive device *(pg. 31 last §-pg. 32 §1-2).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use a public key of either data send/receive device as the data for verification data generation as taught by *Schneier.* One of ordinary skill in the art would have been motivated to perform such a modification in order to allow communicated parties to solve a key-management problem *(Schneier, 32 § 2).*

32. Claims 9-12, 21-24, 33-35 and 38-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Schneier (Bruce Schneier, "Applied*

Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457) and in further view of *Davis et al. (U.S. Patent No. 6775770)*, *Narayanaswami (U.S. Pub. No. 20010013890)* and *Lin (U.S. Pub. 20020025046).*

33. As per claim 22 *Vainio* teaches a key exchange process wherein one of the devices sends information to another device and wherein the information is used to create a symmetric encryption key *(Fig. 5). Vainio* does not explicitly disclose that the authentication process precedes the key exchange process. However, *Vanio* teaches that authentication ensures the identity of a user. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to exchange keys after the users are authenticated. One of ordinary skill in the art would have been motivated to perform such a modification in order to avoid Man-in-the Middle Attack *(Schneier, pg. 48-49).*

Vainio also does not teach each of the terminals transmitting the symmetric key Kc to the personal computer of each user, and thereafter both the personal computers sending and receiving data in cipher according to the symmetric key Kc. *Schneier* teach two computers sending and receiving data in cipher using symmetric key *(Schneier, pg. 28, § 1-2)* and teaches that exchanging the cipher key should be done using other communication channels than cipher data exchange *(Schneier, pg. 176, last three §-pg. 177, first two §)*. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to employ *Vanio's* teaching to transmit the symmetric key to computers sending and receiving data in cipher according to the symmetric key Kc as taught by *Scheneir.* One of ordinary skill in the art would have been motivated to perform such a modification in order to avoid eavesdropping *(Schneier, pg. 176, § 8).*

Vainio does not teach the portable terminal of each user being connected to a personal computer of each user being connected by a secure communication path.

Narayanaswami teaches a terminal being connected to a personal computer by a secure path *(high speed USB, Narayanaswami [31].)* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to connect a portable terminal of each user to a personal computer of each user as taught by *Narayanaswami.* One of ordinary skill in the art would have been motivated to perform such a modification in order to allow rapid transfer of data *[Narayanaswami, 31]).*

Davis et al. teach a secure path *(Davis et al., Abstract).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to connect a portable terminal of each user to a personal computer of each user as taught by *Davis et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to provide to the secure transfer of sensitive information *(Davis et al., Abstract).*

34. As per claim 21 *Vainio* does not teach a secret key being created by a personal computer of each user. *Lin* teaches that computing power, memory capacity and supply power of the portable device may not be sufficient for key generation *(Lin, [21]).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify *Vainio's* invention so that the keys Kc are generated by the personal computers. One of ordinary skill in the art would have been motivated to perform such a modification in order to move key generation into the higher power and memory capacity devices.

35. Claims 9-12, 23-24, 33-35 and 38-42 are substantially equivalent to claims 21-22; therefore claims 9-12, 23-24, 33-35 and 38-42 are similarly rejected.

36. Claims 9-12, 21- 24, 33-35 and 38-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Vainio (Juha T. Vainio, "Bluetooth Security")* in view of *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457).*

37. *Vainio* teaches that Bluetooth can be implemented in any device, including a laptop and a mobile phone (pg. 2 last §). In the broadest interpretation of portable terminal and personal computer some of these devices meet the definition of both. As a result the applicant's invention may involve just two devices where the terminal part of the device (keyboard, display etc.) is a portable terminal, which communicates with the personal computer part, and as such *Vainio's* teaching reads on claims 9-12, 21- 24.

Conclusion

Prior art considered but not relied upon:

Bright *(U.S. Patent No. 5146497)*

Schlafly et al. *(U.S. Patent No. 5297208)*

Dutta et al. *(U.S. Pub. No. 20020186845)*

Bajikar *(U.S. Pub. No. 20020194500)*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Signature

12/20/04

Date

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100